

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act)	CC Docket No. 96-115
of 1996;)	
)	
Telecommunications Carriers' Use of Customer)	
Proprietary Network Information and Other)	
Customer Information)	
)	
Petition for Rulemaking to Enhance Security and)	RM-11277
Authentication Standards for Access to Customer)	
Proprietary Network Information)	

**COMMENTS OF THE UNITED STATES
INTERNET SERVICE PROVIDER ASSOCIATION (US ISPA)**

Marc Zwillinger
Christian Genetski
Sonnenschein Nath & Rosenthal LLP
1301 K Street, N.W.
Suite 600, East Tower
Washington, D.C. 20005
(202) 408-6400

Counsel to US ISPA

Dated: April 28, 2006

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act)	CC Docket No. 96-115
of 1996:)	
)	
Telecommunications Carriers' Use of Customer)	
Proprietary Network Information and Other)	
Customer Information;)	
)	
Petition for Rulemaking to Enhance Security and)	RM-11277
Authentication Standards for Access to Customer)	
Proprietary Network Information)	

**COMMENTS OF THE UNITED STATES
INTERNET SERVICE PROVIDER ASSOCIATION (US ISPA)**

The United States Internet Service Provider Association ("US ISPA"),¹ through its undersigned counsel, respectfully submits its comments to the Federal Communications Commission's ("Commission") Notice of Proposed Rulemaking ("NPRM") released February 14, 2006 (FCC 06-10) in the above-captioned proceedings. The Commission released the NPRM in response to a Petition for Rulemaking filed by the Electronic Privacy Information Center ("EPIC").²

¹ US ISPA is a national trade association that represents the common policy and legal concerns of the major Internet service providers ("ISPs"), portal companies, and network providers. US ISPA is comprised of AOL, AT&T, BellSouth, Earthlink, Microsoft, SAVVIS, United Online, Verizon Online Services, and Yahoo!.

² Petition of the Electronic Privacy Information Center for Rulemaking To Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005) ("EPIC Petition").

The members of US ISPA take seriously the protection of customer information.

US ISPA believes, however, that the Commission should limit the scope and applicability of any rules requiring the implementation of EPIC's proposed security controls to exclude application of such rules to Internet Service Providers ("ISPs"). Requiring ISPs to implement all of the controls suggested by EPIC would be extremely costly and burdensome for ISPs, because: (1) the definition of Customer Proprietary Network Information ("CPNI") in Section 222(h)(1)(A) has never before been applied to cover data and records of ISPs and does not translate well to records related to Internet activity, making it unclear how ISPs would implement rules designed to address dissimilar information; (2) ISPs have already established their data handling practices pursuant to different rules, such as the Electronic Communications Privacy Act, 18 U.S.C. § 2701, et. seq., ("ECPA"), as well as the terms of their customer contracts.

I. The Scope of Any New CPNI Rules Should Be Limited

The Commission's authority to regulate the handling of CPNI is rooted in Section 222 of the Communications Act of 1934, as amended ("Act"), which has not historically been applied to ISPs. In fact, the definition of CPNI in § 222(h)(1) clearly does not contemplate ISP records. Section 222(h)(1)(A) concerns information related to the "quantity, technical configuration, type, destination and amount of use in a telecommunications service" and § 222(f)(1)(B) is limited to "[i]nformation contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." These definitions have little application in the context of the Internet, where configuration and destination information is passed publicly over the Internet, where records of Internet connections are not ordinarily maintained for billing purposes nor provided to customers, and where such information is the subject of a separate federal statutory regime.

This narrow focus of the CPNI definition is further reflected in the concerns raised in the EPIC petition giving rise to the instant proposed rulemaking, which centered specifically on attempts by data brokers to access *consumer telephone call records* without authorization. Indeed, in the NPRM, the Commission included several pages of detailed questions related to specific carrier experiences and practices in connection with the telephone toll records of telephone subscribers. Amidst these issues, in a single sentence in a sub-paragraph related to breach notification, the Commission sought comment on whether any requirements adopted by the Commission should include both Voice over IP (“VOIP”) services and other IP-enabled service providers, such as ISPs.³ The NPRM acknowledges, however, that the issue of the scope of the Commission’s jurisdiction generally to regulate VOIP and IP-enabled services is being addressed in another Commission proceeding.⁴ Given the narrow focus of this rulemaking on telephone toll records of consumers and traditional CPNI, US ISPA strongly urges the Commission not to use this rulemaking to begin a novel endeavor of analogizing the CPNI rules to ISP records that were neither described or contemplated in Section 222 of the Act.

Extension of this CPNI rulemaking to include ISP records would be inappropriate for several reasons. First, ISP records were not identified as targets of the call pretexting attempts that, at least in part, generated this proceeding. Second, ISPs do not typically segregate billing and customer records in the manner contemplated by § 222(h)(1)(B) or the EPIC Petition, nor can ISPs easily segregate such records given their range of IP-enabled service offerings, including electronic mail, web hosting, and instant messaging, only some of which contain a

³ *Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Notice of Proposed Rulemaking, FCC 06-10, ¶ 28 (rel. Feb. 14, 2006) (“NPRM”). This question did not appear specifically on the published Federal Register notice.

⁴ *IP-Enabled Services*, Notice of Proposed Rulemaking, 19 FCC Rcd. 4863 (2004)

voice component.⁵ Given the variety of services provided by ISPs, ISPs should not be required to protect all customer information in accordance with rules formulated by the Commission in order to protect calling/billing records of voice customers.

Third, the information pertaining to customers of IP-enabled services is already protected and regulated by a number of federal statutes, most notably ECPA, which provides a complex statutory regime for protecting records related to customers or subscribers of ISP services.⁶ In the case of ISPs, the proposed set of regulations designed to protect CPNI will likely overlap or conflict with ECPA's carefully conceived statutory provisions protecting ISP customer information, creating an unnecessary and confusing duplicate layer of regulation.⁷ Over the years, ISPs have devoted considerable resources to develop programs to ensure compliance with the regime set forth in ECPA, but have not established procedures or systems with CPNI rules in mind.

Finally, many, if not all of the ISPs, already have privacy policies in place that protect consumers' personally identifiable information. These privacy policies are subject to Federal Trade Commission ("FTC") jurisdiction and enforcement action. In fact, the FTC has brought several recent enforcement actions against companies that have breached their privacy policies. Moreover, the FTC has recently announced plans to actively investigate and enforce violations of its consumer protection laws/regulations by broadband Internet access providers who offer such services on a non-common carrier basis. Similarly, for ISPs providing services to business

⁵ Should the Commission extend this rulemaking proceeding to impose regulations on VOIP providers, such regulations should be limited to only customer information specifically related to the provision of VOIP services, and the Commission should make clear that the provision of VOIP service by an ISP shall not cause data pertaining to other subscribers, or other data pertaining to the VOIP subscriber, to be covered by the Commission's CPNI regulations.

⁶ 18 U.S.C. §§ 2701 - 2706

⁷ Although US ISPA members are not providers of cable television services, information related to customers of Cable ISPs are also covered to some extent by the Cable Act, 47 U.S.C. § 551.

customers, any customer information is considered confidential and is also subject to contract negotiations between the parties. Thus, there is no separate need for the Commission to impose its CPNI rules on ISPs.

Accordingly, US ISPA believes that any rules the Commission chooses to implement should steer well clear of the statutory regime set forth in ECPA, and that the Commission should carefully limit the scope of any new rules to prevent the creation of burdensome and costly regulations that would not solve the issues that the CPNI rulemaking seeks to address.

II. EPIC's Specific Recommendations

The Commission seeks comments on EPIC's proposal to impose rules requiring covered entities to implement security controls by, among other things, limiting data retention and providing notice to customers in advance of the release of CPNI, and if their CPNI is breached. Imposing rules in these areas would impose significant burdens on ISPs that may in many cases conflict with existing legal obligations.

A. Limits on Data Retention

EPIC proposes that the Commission should implement rules requiring customer call records to be deleted as soon as they are no longer needed for billing or dispute purposes;⁸ or, alternatively, that providers should be required to de-identify call records (so that call records can be maintained for data analysis without being matched to identification data).⁹ US ISPA opposes the application of any such rules to ISPs for the reasons discussed below.

⁸ Significantly, there are varying state statutes of limitations regarding contract disputes, which means that ISPs must store customer information for a certain period of time to ensure that the information is available in the event a dispute arises.

⁹ NPRM at ¶ 20.

First, many US ISPA members provide services for free, and thus do not maintain any records for billing or for dispute purposes, but do maintain various types of records regarding a user's Internet activity either at the user's direction (email archives, Buddy Lists, frequently visited websites) or by automatic operation of log files required for security and authentication purposes. Other records are maintained pursuant to the privacy policies between the users and the ISPs. More often than not, rather than seeking record destruction to protect users, the government has sought to encourage ISPs to retain existing data longer in order to aid law enforcement investigations of users.¹⁰ Moreover, ISPs are subject to the data preservation requirements in the Stored Communications Act (18 U.S.C. §2703(f)) and are routinely compelled to preserve customer information in response to law enforcement requests. Thus, any rules the Commission imposes requiring providers to dispose of CPNI after a certain period of time may not only impose a significant burden on ISPs, but it also might affect their security practices, and conflict with the requirements of the Stored Communications Act and the needs of law enforcement.

B. Notice

In its petition, EPIC also proposes that the Commission implement rules requiring providers to notify customers through out-of-band communications, such as telephonically, as a prerequisite to releasing CPNI, or subsequently, in situations where CPNI may have been breached.¹¹ Notification rules involving multiple methods of communication would not be workable for ISPs whose only method of communication with many if not most users is via email. US ISPA also opposes the implementation of any industry-specific breach notification

¹⁰ Although US ISPA does not endorse mandatory data retention, US ISPA does support the ability of ISPs to maintain records consistent with their internal policies, practices and business needs.

¹¹ NPRM at ¶ 21.

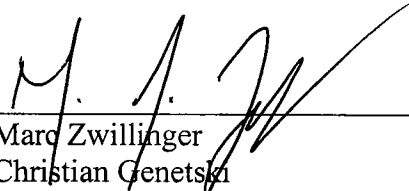
rules, as such rules will likely create a set of standards that conflict with state data breach notification laws already in force. At least twenty-three states have already enacted such laws, which require businesses to notify customers if sensitive data that could be used for identity theft purposes is obtained by an unauthorized person. US ISPA members have already invested considerable resources to create and implement compliance programs designed to respond to data breaches in accordance with this multitude of sometimes inconsistent state laws. Creating an additional notice regime solely for CPNI that differs from the rules imposed by state laws for other types of sensitive data would be cost-intensive and unlikely to yield measurable benefit beyond that ensured by existing state data breach laws. Rather than any breach notification regulations that could be promulgated by the Commission, US ISPA supports federal legislation that would preempt state laws and would provide a uniform standard for the appropriate data categories and circumstances under which companies should provide notice to customers in the event of a security breach.

III. Conclusion

In view of the foregoing, US ISPA members believe that the Commission should limit the scope and applicability of any rules requiring the implementation of EPIC's proposed security controls to exclude application of such rules to ISPs. As these comments demonstrate, putting costly and unnecessary requirements on ISPs would create a substantial burden, especially when the need for applying CPNI requirements to the data and records of ISPs has not been established. ISPs already comply with a number of regulations relative to customer information, have established practices for handling customer data pursuant to these rules, and where applicable, protect information pursuant to the terms of their customer contracts. The confidentiality and protection of customer data is vitally important to all US ISPA members and

the creation and extension of additional requirements to ISPs by the Commission would be misguided.

Respectfully submitted,



Marc Zwillinger
Christian Genetski
Sonnenschein Nath & Rosenthal LLP
1301 K Street, N.W.
Suite 600, East Tower
Washington, D.C. 20005
(202) 408-6400

Attorneys for US ISPA

Dated: April 28, 2006